DevOps Shack

TRIVY

[Click Here To Enrol To Batch-5 | DevOps & Cloud DevOps]

Trivy Documentation

Trivy is an open-source vulnerability scanner for containers and other artifacts, developed by Aqua Security. It helps users discover vulnerabilities in their container images and filesystems.

Installation Steps:

Before installing Trivy, ensure that your system meets the following requirements:

- Running a supported Linux distribution.
- Internet access to download packages.
- `wget` and `apt` package manager installed.

Step 1: Install Dependencies

Run the following command to install necessary dependencies:

```
sudo apt-get install wget apt-transport-https gnupg lsb-release
```

Step 2: Add Trivy Repository Key

Add the Trivy repository key to your system's trusted keyring:

```
wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | gpg --dearmor | sudo tee /usr/share/keyrings/trivy.gpg > /dev/null
```

Step 3: Add Trivy Repository

Add the Trivy repository to your system's list of package sources:

```
echo "deb [signed-by=/usr/share/keyrings/trivy.gpg]
https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -sc) main" |
sudo tee -a /etc/apt/sources.list.d/trivy.list
```

Step 4: Update Package Lists

Update the package lists to include the newly added Trivy repository:

```
sudo apt-get update
```

Step 5: Install Trivy

Finally, install Trivy using the following command:

```
sudo apt-get install trivy -y
```

Trivy Usage Guide

Trivy is a powerful vulnerability scanner for containers and filesystems. This guide will walk you through the various ways to use Trivy for scanning folders and Docker images.

Folder Scan

To scan a folder or directory for vulnerabilities, use the following command:

```
trivy fs path_to_scan
```

Example:

```
trivy fs /path/to/scan
```

To save the scan result in HTML format, use the `--format` and `-o` options:

```
trivy fs --format html -o result.html path_to_scan
```

Example:

```
trivy fs --format html -o result.html /path/to/scan
```

You can also specify the types of security checks to perform using the `--security-checks` option:

```
trivy fs --format html -o result.html --security-checks vuln,config
Folder_name_OR_Path
```

Docker Image Scan

To scan a Docker image for vulnerabilities, use the following command:

```
trivy image image_name
```

Example:

```
trivy image my_image:latest
```

To save the scan result in HTML format, use the `-f` and `-o` options:

```
trivy image -f html -o results.html image_name
```

Example:

```
trivy image -f html -o results.html my_image:latest
```

You can specify the severity levels of vulnerabilities to include in the report using the `--severity` option:

```
trivy image -f html -o results.htm --severity HIGH,CRITICAL image_name
```

Example:

```
trivy image -f html -o results.html --severity HIGH,CRITICAL
my_image:latest
```

Conclusion

Trivy offers comprehensive scanning capabilities for both folders and Docker images, providing valuable insights into potential vulnerabilities. By integrating Trivy into your development and deployment workflows, you can ensure the security of your containerized applications. For more advanced usage and options, refer to the Trivy documentation.

Additional Resources:

- Trivy GitHub Repository
- Trivy Documentation
- Aqua Security Website